Journal of Information Systems Engineering and Management
2025, 10(29s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Comprehensive Review of Cryptography and Steganography Algorithms

Ms. Halima Abbas Ahmed[1], Dr. Asmaa Mahfoud[2*], Dr. Omar Ismael Al-Sanjary[3]
[1] *Post Graduate student in the School of Graduate studies, Management & Science University, Shah Alam Malaysia. halimasaline2019@gmail.com*
[2] *Senior Lecturer in the Faculty of Information Sciences & Engineering, Management & Science University, Shah Alam Malaysia, Malaysia. asmaa@msu.edu.my*
[3] *Associate Professor of Computer Center, University of Mosul, Mosul, Iraq. dr.omar.ismael@uomosul.edu.iq*

ARTICLE INFO

Received: 28 Dec 2024

Revised: 18 Feb 2025

Accepted: 26 Feb 2025

ABSTRACT

During recent decades, the utilization of digital communication has played a fundamental role across various industries such as healthcare, banking, and information technology corporations. All data that is transmitted via the Internet requires a high level of protection to ensure safe transmission of the original data from the source to the intended destination. Cryptography and information hiding techniques have emerged as two key components for protecting sensitive data and communication channels, providing another layer of security. This paper explores the benefits and challenges associated with the combination of cryptography and steganography and identify the potential vulnerabilities of current image steganography techniques and improve overall security of covert communication systems. Cryptography and Steganography provide a multi-layered defense against prospective threats. Encryption protects the privacy of information, whereas steganography adds another layer of obscurity, making it difficult for adversaries to identify and intercept sensitive data. Moreover, Cryptography and information hiding have many applications in the contemporary day, including the security of confidential financial data and the protection of secret government records. Considering the rapid growth of electronic communication and the escalating volume of data communicated over the Internet, there is an urgent need for robust encryption and data concealment methods. As a result, this integration satisfies the requirements of capacity, security, and robustness for secure data transmission over an open channel.

Keywords: System Security, Data Transmission Security, Steganography. Cryptography Image Compression

INTRODUCTION

Due to advancements in information and digital communication, there is a need for secure data transmission over the Internet, which requires high levels of security and confidentiality [1]. Additionally, this includes protecting data from unauthorised access by malicious actors like hackers [2]. Notably, the complexity of security systems is increasing with the integration of various technologies aimed at securing sensitive information, reliability, and accessibility [2]. Information system security is categorised into two categories: encryption and information hiding. These technologies are reliable to ensure the increasingly required information security in data transmission and storage, but their techniques differ[3]. Cryptography is a key element in numerous security systems, serving to protect the confidentiality of sensitive information [4]. Encrypting data makes it unreadable to people without the appropriate decryption key, guaranteeing that only authorised people can access the data [5]. Cryptography has its origins in ancient Egypt [6], where basic substitution ciphers were employed to protect messages [3]. The emergence of the computer era has rendered cryptography a vital instrument for protecting confidential data in the realm of digital technology [7].

Information hiding is another important technique in security systems, providing a way to protect the integrity of data [1]. By embedding a hidden message within another file, it becomes possible to verify that the data has not been tampered with without revealing the hidden message to unauthorised parties [8], [9]. Information hiding, a relatively newer field, has its origins in the early 20th century [10]. It initially was used primarily for artistic purposes, such as

hiding a secret message within an image or audio file. However, in recent years, data hiding has become increasingly important to securely, store, and transmit sensitive information [11]. Steganography is one of the most common digital information-hiding applications, whereby a hidden message is embedded within another file [12]. Another application of information hiding is watermarking, whereby a hidden message is embedded within an image or audio file, allowing the owner of the file to prove ownership and prevent unauthorised copying [1], [8]. Digital watermarking can be divided into visible and invisible types, serving several purposes, including protecting copyright ownership [13]. Figure 1 illustrates a general digital information security system's classification tree [7], [14].

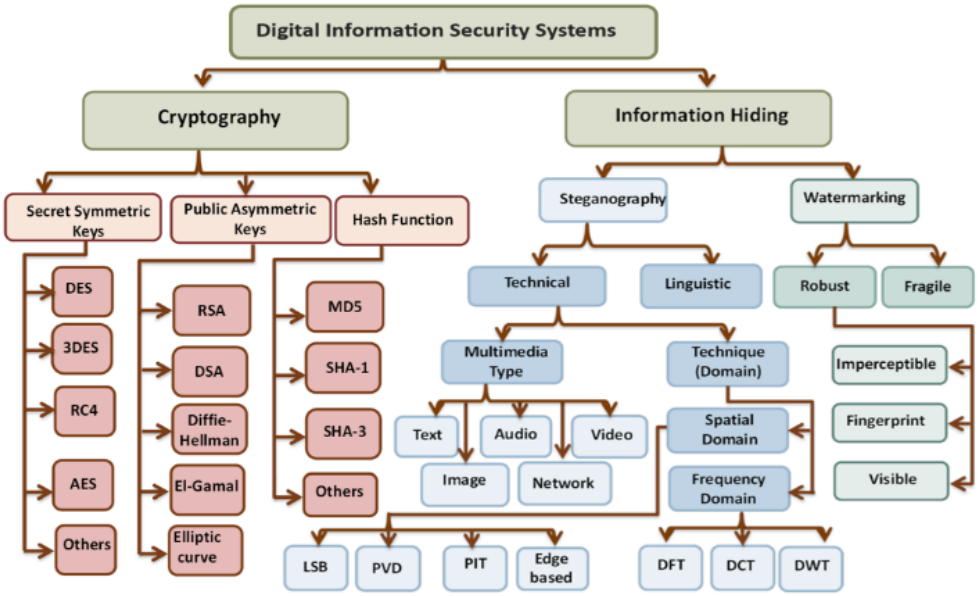

Figure 1. Classification tree of security systems

CONCEPT OF CRYPTOGRAPHY AND STEGANOGRAPHY

Cryptography and steganography are distinct concepts that are often used in combination to protect and transmit sensitive information securely[4].

A. Overview of Cryptography

Cryptography is the art of secret writing that converts data into an unreadable format [1]. , protecting confidentiality over public networks [15]. It involves transforming plaintext into ciphertext, which only individuals with a secret key can decrypt [16]. Decryption reverses this process, converting unreadable cipher text to plaintext [17]. A cryptosystem consists of finite potential plaintext, cipher text, keys, and encryption and decryption techniques. Cryptography is closely linked to cryptology and cryptanalysis [18]. which involves techniques for decrypting messages without knowing the encryption details [7]. Cryptology is the combination of cryptography and cryptanalysis [17], [19].

- *Security Function of Cryptography.*

According to Ashari et al. (2022) and Taha et al. (2019) Cryptography offers security benefits such as confidentiality, data integrity, non-repudiation, and authentication. Confidentiality ensures that information is kept secret and only authorized parties can access it [22] Data integrity guarantees that digital information is not corrupted, and only authorized parties can access or modify it [21] non-repudiation shows that a user performed an action and prohibits disputing it [22]. Authentication ensures identity identification and verification of an entity [21]. Cryptography primitives, as presented in Table 1. an array of tools and procedures that are essential to the field of Cryptography [6]. These primitives can be selectively employed to confer a range of security services as desired. Among the key primitives are encryption, Authentication Codes for Messages (MAC), Hash functions, and Electronic Signatures [6], [23].

Table 1. Security Services and Their Fundamentals

Confidentiality	
Encryption	✓
MAC	×
Hash functions	×
Electronic Signatures	✓
Data Integrity	
Encryption	×
MAC	✓
Hash functions	Possibly
Electronic Signatures	✓
Non- repudiation	
Encryption	×
MAC	Possibly
Hash functions	×
Electronic Signatures	✓
Authentication	
Encryption	×
MAC	✓
Hash functions	×
Electronic Signatures	✓

- *Classifications of Cryptographic algorithm.*

There are several approaches for classifying cryptographic algorithms. that will be sorted based on the number of keys used during encryption and unscrambling, and assisted, described by their request and use. Modern cryptographic algorithms can be divided into three broad categories Symmetric-key cryptography, public-key (asymmetric-key) cryptosystems, and hash functions. Figure 2 Illustrates modern cryptography algorithms [14], [24], [25]. In most cryptographic systems, both symmetric and asymmetric algorithms (and occasionally hashing) are employed together, which is known as hybrid cryptography [22]. Hybrid cryptography refers to the integration of many algorithms with the objective of enhancing efficiency and performance, as well as addressing the limitations inherent in individual algorithms [26].

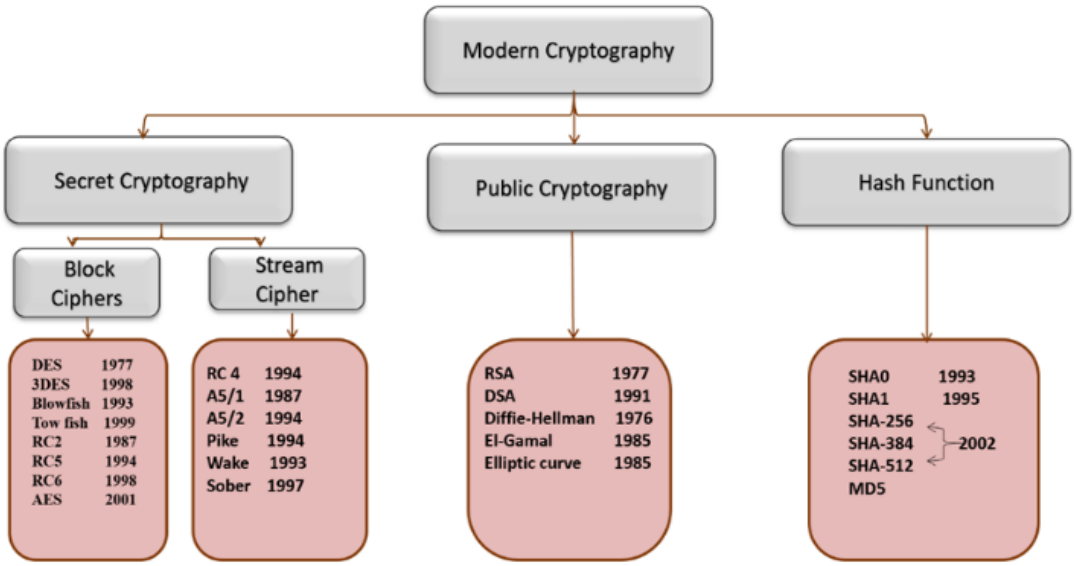

Figure 2. Categorization of modern cryptographic algorithms

- *Cryptography Using Private/Secret/Symmetric Keys.*

Symmetric-key cryptography is a cryptographic technique that employs a single key for both the encryption and decryption of a message [25]. To ensure the security of the encrypted data, the same key is shared between the communicating parties and must be kept confidential [17], [21]. Figure 3. illustrates Symmetric private-key encryption system. The efficiency of this algorithm is notable in terms of both speed and computing power due to its implementation of a single key [26].

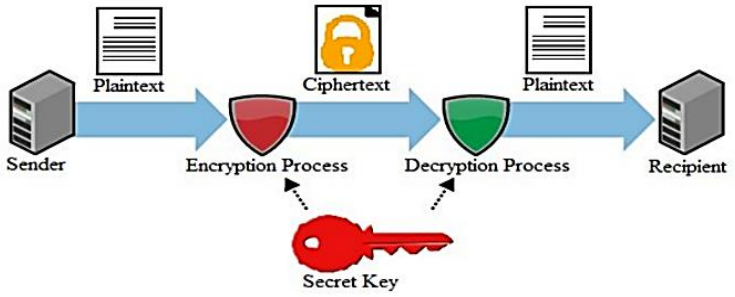

Figure 3. Symmetric private-key encryption system [27]

The encryption algorithm utilized in symmetric-key cryptography operates on either a stream of data or fixed-size blocks of data [21]. A block cipher is designed to function on groups of bits that have fixed lengths, which are referred to as blocks. In contrast, a stream cipher operates continuously on each element of plaintext and generates one element at a time as it progresses [28]. The key, which usually consists of a sequence of arbitrary bits, is employed as input to the encryption algorithm to convert the original message (plaintext) into an encrypted message (ciphertext) [29]. During the decryption process, the same key is utilized in reverse to convert the ciphertext back into plaintext [29]. There are several widely used symmetric-key cryptographic algorithms, including Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES), Rivest Cipher (RC) Series, and Blowfish schemes [25], [26], [29]. Whereas AES symmetric-key cryptography is widely used for various applications, including secure communication, data storage, and file encryption Hazzaa et al. (2021); Reis et al. (2022).

- *Public Key Cryptography/Asymmetric Cryptography.*

Asymmetric/Public Key encryption and decryption use distinct keys mostly used for authentication, non-repudiation, and key exchange. For data protection, these algorithms employ two distinct keys, one utilized by the transmitter and the other by the recipient [30]. Some of these two keys may be shared by communication parties Figure 5. Because one of the two keys used in such algorithms is publicly known and used by the sender, these methods are vulnerable to mathematical and other related attacks. An attacker starts such assaults and attempts to obtain the receiver side key using knowledge of the public key (private key) [21]. Asymmetric algorithms become less efficient because of the production of these two keys. Moreover, numerous public key encryption techniques exist, including but not limited to RSA (Rivest, Shamir, and Adleman), DSA, Rabin, Elgamal, Diffie-Hellman and Elliptic curve cryptographic algorithms [23].

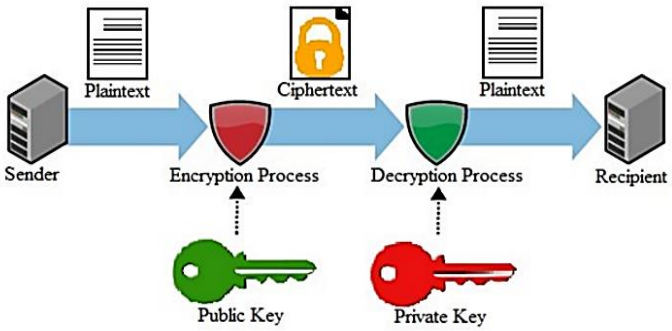

Figure 5. Public-key encryption system (Faheem et al., 2017)

- *Hash Function*

The hash function is a critical component that offers a message authentication service to authenticate and maintain the integrity of data [31]. There are several Hash algorithms like SHA1 (Secure Hash Algorithm 1), SHA-2 (Secure Hash Algorithm 2) family, which includes SHA256, SHA384, and SHA521 and MD5 (Message Digest 5) [32], [33].Irrespective of the length of the message input, the hash function receives an input and performs a computation resulting in hash value or a message digest of a predetermined length [34]. The underlying concept of this mechanism is to produce a distinct digital signature of the message that can be employed with efficacy and efficiency to prevent data duplication. Thus, each message has a distinct message digest that guarantees its uniqueness. The hash function exhibits various attributes, such as the property of being a one-way function, where the output is transformed in a non-reversible manner from the input. Additionally, the hash function must have the capability to process input data of any size [34], as illustrated in Figure 6. Furthermore, the algorithm generates an output of a predetermined size, and its computational efficiency makes it suitable for processing any given input. Notably, any alteration made to the input data will generate a distinct hash value, and offering multiple inputs into the hash function will produce a multi-hash value output [32]. There exist numerous objectives.

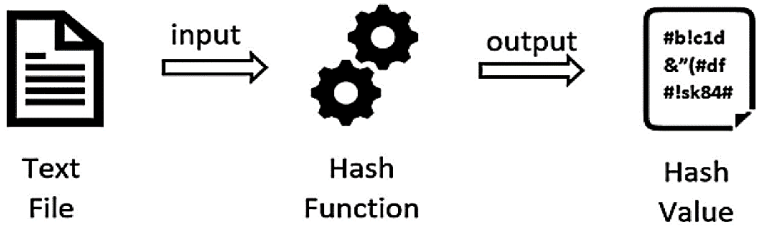

Figure 6. Hash function process [34]

For the utilization of hashing, including facilitating the comparison of voluminous amounts of data or generating a fixed length output to enable facile comparison of the hash value as opposed to the entire dataset [32]. Additionally, hashing simplifies the avoidance of data duplication in databases and supports record retrieval, rendering the hash function an efficient means of storing passwords [32].

B. Overview of Steganography

Steganography is a combination of Greek words for cover and writing [15], [35] , originated in ancient Greece when secret messages were tattooed on the shaved heads of slaves and transmitted when their hair grew back [10]. This technique was later used in wax tablets during the First World War and microdots during the Second World War [10]. Today, steganography is considered a modern tool for secure communication, embedding secret information in a cover to ensure its undetectable existence [15]. The medium used to conceal the information is common text, picture, audio, or video, known as a cover image [36]. The cover media after embedding is known as the "stego-medium." A secret key can also be used to ensure extraction method security, making it more difficult for unauthorized individuals to extract information (Alyousuf et al., 2020).

- *Fundamental Elements of Steganography.*

According to Alyousuf et al. (2020) ; Ramakrishnan, (2018), (2018) stated that the basic elements of steganography include the secret message being the message that will be embedded, and the cover image containing a hidden message. A steganography algorithm is employed to embed a message inside a cover image, while an extracting steganography algorithm is used to retrieve the hidden message from the steganographic image [37], [38]. Key data is required for embedding and extracting procedures [37]. Murugan & Uthandipalayam Subramaniyam, (2020) explained that steganography is primarily a technique for concealing information in cover medium and producing stego-images. The sender sends a stego-image to the collector over a known medium, but the intruder is unaware that the stego-image conceals the message [40]. Upon entering the collector side, a stego-image concealed message can only be erased using the stego-key (depending on the embedding algorithm) [37]. The concept of image steganography is depicted in Figure 7, where the embedding process needs an image (cover) to be associated with the message (secret).

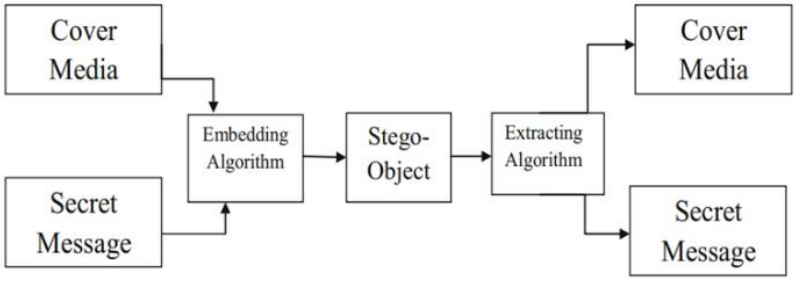

Figure 7. Steganography concept diagram Murugan & Uthandipalayam Subramaniyam, (2020)

- *Classification of Steganography.*

Steganography can be categorized into technical and linguistic approaches[7], as shown in Figure 8, with technical steganography being further divided into two categories based on the type of multimedia and technique used [7], [41]. The main challenge in steganography is maintaining image quality while carrying a large amount of payload, as massive amounts of hidden data can reduce the quality of images that can detect data [7]. There are five primary file formats available for multimedia steganography.

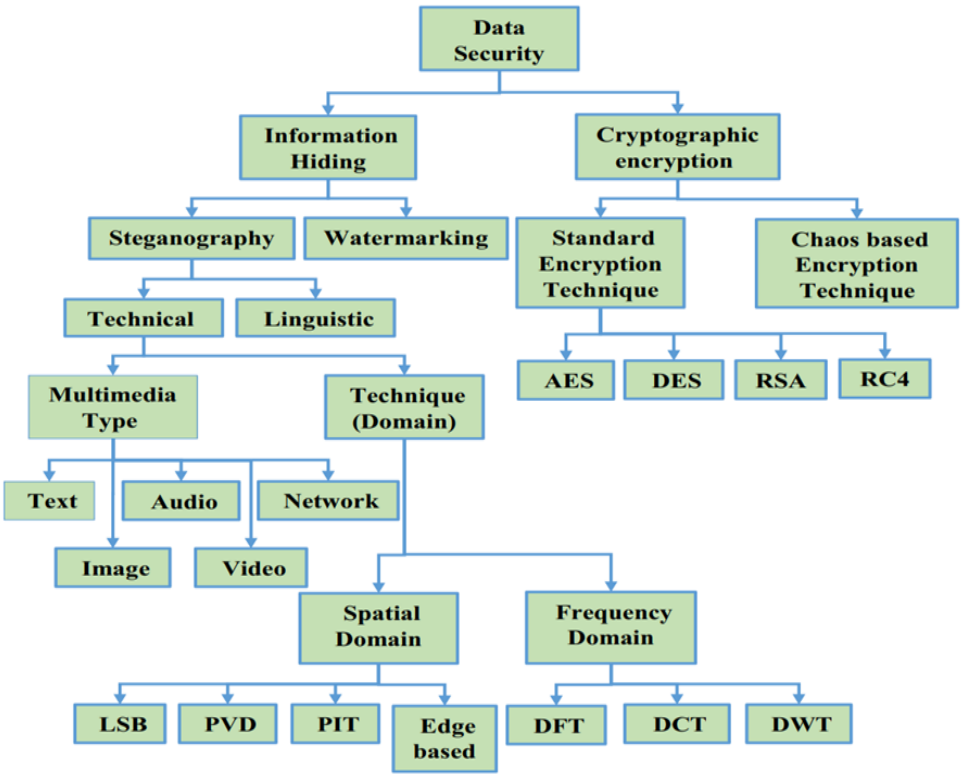

Figure 8. Steganography Approaches [7]

a. **Text steganography:** it is a technique that conceals hidden information within text files, reducing memory usage. It uses white spaces, tabs, and capital letters to hide messages, but is uncommon due to text files often containing redundant content [15].

b. **Image Steganography** Digital images are commonly used as cover media in steganography systems due to the availability of automated image data and the rise in internet speed distribution [12]. Secret information is encoded in cover images using an algorithm based on a steganographic key. The stego-image is sent to the intended recipient, who uses an extraction method to decipher the concealed information. This ensures that only unauthorized individuals can access communication, not the hidden secret message sent through images [24].

c. **Audio steganography:** Audio steganography involves concealing hidden information within audio covers using effective embedding methods, ensuring security and robustness against attacks. Existing algorithms

primarily embed secret information in WAV and MP3 sound files, ensuring that intruders cannot access the data. [6].

d. Video Steganography: A video file is used as the cover object, and MP4, MPEG, or other video formats are supported.to embed secret data invisible to the human eye, with video having greater embedding capacity than digital images [24].

e. Network and Protocol Steganography: The secret information is encoded utilising network control protocols such as HTTP, FTP, TCP, SSH, and UDP, among others., while Voice-over-IP incorporates confidential data, making protocol steganography a more secure level [12], [42].

f. Evaluation Criteria for a Steganography Scheme: The effectiveness of a steganographic system is evaluated based on its capacity, imperceptibility, and security, with capacity and security being reciprocal. [43]. Robustness is another important attribute [10], [44] , as shown in Figure 9. As capacity increases, security decreases, and vice versa [45].

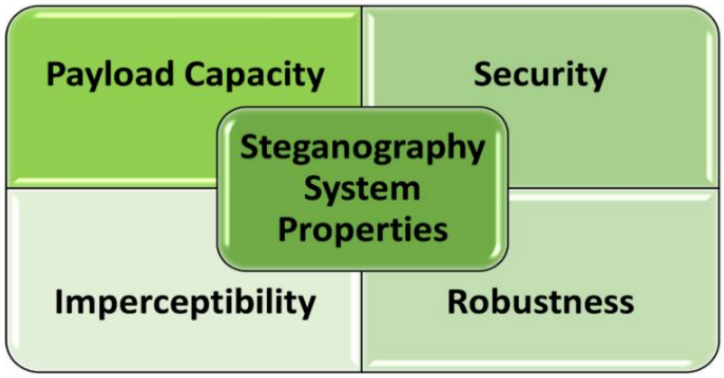

Figure 9. Principal Steganography System Attributes [44].

While Ramakrishnan(2018) mentioned that there are seven properties, the same as the previous properties, along with Embedding Rate, Indistinguishability or Fidelity, and Type of Supported Images. The subsequent section elaborates on the qualities discussed in greater detail:

a. Capacity is the amount of information that can be easily stored and retrieved from a cover medium without having to change the cover medium.

b. Imperceptibility: There should be no visual difference between the cover and the stego -object, i.e., the inserted message should not be visible to the human eye.

c. Security: A data installation procedure is deemed secure if the inserted data cannot be removed following identification by an eavesdropper. It is contingent upon the knowledge of the embedded algorithm and mystery key.

d. Robustness: A stego structure is robust if it can withstand any kind of attack and any kind of change, such as scaling, rotation, filtering, and lossy pressure, among others.

e. Embedding Rate: It is often provided in absolute measurement, such that the length of the secret message or, in relative measurement, information insertion rate, is given in bits per nonzero DCT (Discrete Cosine Transform) pixel coefficient (BPNPC) and bits per pixel (BPP).

f. Indistinguishability or Fidelity: Under the same level of protection and restriction, it is expected that Stego-images will not contain any visual anomalies. The higher quality of stego-images implies more blurriness.

g. Types of Supported Images: Understanding the appropriate photo formats for steganography is crucial, as image quality impacts the steganographic methods that can be employed with it, irrespective of the compression method used.

- *Image Steganography Basic.*

Steganography hides multimedia information, including text, images, audio, video, and networks. It can be categorized into spatial domain and frequency domain techniques [11] as indicated in Figure 10. Furthermore, Ahmed (2021) added that image steganography uses various methods, including spatial domain, transform domain, spread spectrum, and patchwork. These techniques aim to achieve security.

a. Spatial Domain Technique: information is added directly into the intensity of the original image's pixels [46]. This method depends on the format of the image used as the cover material. For data concealment, this technique directly modifies some bits into the pixel values of the image [47]. There are numerous categories of widely employed spatial domain approaches, including Least Significant Bit (LSB) substitution, Pixel Value Differencing (PVD), Exploiting Modification Direction (EMD), etc. However, LSB is the easiest and simplest [48].

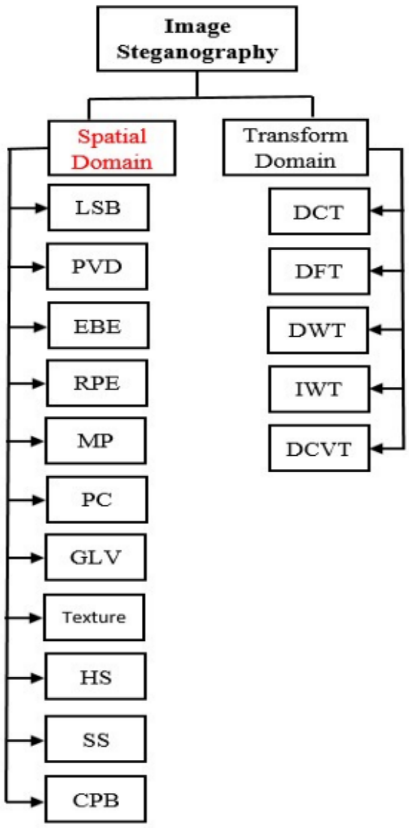

Figure 10. Classification of image Steganography [11]

b. Transform or Frequency Domain: This-steganography- domain-is-used-to-mask-huge-amount-of-data. It provides great security, good invisibility, and no communication loss. In this domain, the cover image is modified initially. Then, the hidden message is concealed in strategic locations [8]. The-transform-domain-can-be-divided-into three major categories, including Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) [48]. The-embedding-process-in-this-domain-is-more-complex-than-the-embedding process in the spatial-domain entirely because-the--data-is-not--hidden-directly-in-the-pixel's-intensity,but-rather-in-the-pixel's coefficient. Moreover, it is superior to the image domain because it conceals information in a medium that is less susceptible to cropping and compression. JPEG picture format is the prevalent file format used in this arena, particularly with DCT [8].

c. Spread Spectrum: The spread spectrum is a strategy that disperses secret data throughout the cover image, making it difficult for hackers to detect. This technology creates a stego-image by encapsulating the hidden data in noise before combining it with the cover image. This robustness against intruders makes it impossible for secret information to be viewed [8].

d. Patchwork: It is also referred to as a statistical technique that uses redundant patterns encoding to implant secret information in cover images. The intensity of a pixel can vary between patches, making them invisible to

human eyes. The primary limitation is that only one bit can be implanted, but the image can be subdivided into more bits. The key advantage is that if one patch is destroyed, others remain secure as the secret data is concealed in multiple areas across the image [8].

e. Distortion Technique: This method is-used-to-store-the information-embedded-in-the-signal-distortion. Messages that-have-been-encrypted-can-be-restored-if-the- original- message-is-known-during-decoding. Due to the necessity of comparing the original carrier image and stego-image, this procedure requires knowledge and caution. If the cover image is utilized than once, the-stego-image can be easily identified-by intruders [9].

f. Masking and Filtering: Like the watermarking technique, these methods are used to conceal information by stamping a picture with 24-bit resolution or grayscale type, using software to transmit the message to a larger image area [9].

IMAGE COMPRESSION TECHNIQUES

The primary objective of image compression is to eliminate the user-irrelevant portions of an image. This decreases the image's file size by decreasing the number of pixels, making it more suitable for data storage and transmission [49]. Figure 11 depicts the image compression process in which the image is provided as input to an encoder, which turns the image into bit streams. These encoded streams (bits) are then transmitted to the decoder, which decodes them, and the decoder's output is the final output image [50].

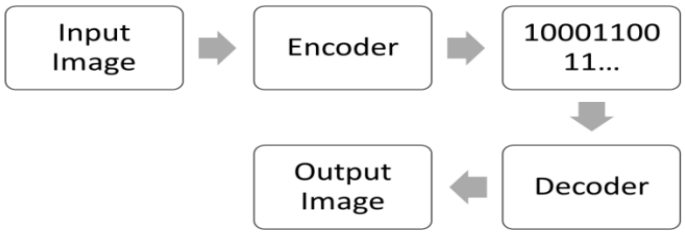

Figure 11. Processing of image compression [50]

Two categories exist for classifying picture compression techniques: Differences between Lossy and Lossless Image Compression [49]. According to Xin & Fan (2021) explained in lossy compression, data is stripped from a file and is not restored to its original state upon decompression. Specifically, data is deleted forever. This data loss is typically imperceptible. Nonetheless, the longer file is compressed, the more deterioration occurs, and the loss becomes obvious over time. On the other hand, after decompression, lossless compression rebuilds and restores file data to its original state. Without data loss, the file can be decompressed to its original state. Furthermore, lossy compression significantly reduces file size in comparison to lossless compression [50]. Lossless compression is typically employed by compressing images, audio, and text. However, lossy compression is used primarily to compress pictures, audio, and video [51]. Also, in lossless and lossy compression, different types of algorithms are utilized to shrink file sizes. Lossless compression algorithms include Run Length Encoding, Lempel-Ziv-Welch (LZW), Huffman Coding, and Arithmetic Encoding, whereas lossy compression employs the methods Transform Coding, Discrete Cosine Transform, Discrete Wavelet Transform, and Fractal Compression [51]. Notably, DCT and DWT are additional image steganography techniques in which the spatial Domain is converted to the frequency domain and the pixel coefficients are employed to conceal the secret data.

COMBINING CRYPTOGRAPHY WITH STEGANOGRAPHY

The integrity of the data may be compromised, manipulated, or even utilized for future malicious activities by unauthorized individuals. An optimal approach for addressing these issues would involve using the benefits of cryptography and steganographic methodologies to construct a hybrid system that surpasses the individual capabilities of each methodology. Whereas both systems can be merged to provide an additional secure level [41]. Additionally, combining cryptography with steganography improves the security of the data, but steganography alone is less safe than the combined method [52]. Once the steganographic pattern is revealed to an unauthorized user, the secret data is susceptible to hacking and modification. Therefore, the message can be scrambled using cryptography to encrypt the provided data. And this encoded communication can then be concealed within a cover medium via steganography [7]. This unified strategy will achieve the three goals of information concealment: security, limitation, and robustness [21].

RELATED LITERATURE

In this study, the most recent publications in the fields of steganography and cryptography have been analyzed with the aim of developing advanced multilayer system's security for confidential communication. This section delves into the various aspects of the research presented and discuss their implications, challenges, and contributions to the field of steganography and cryptography. The following below is an overview of some contemporary and pertinent research studies. In the section on steganographic techniques and challenges, the literature review includes a wide range of steganographic techniques, each with its own power and vulnerabilities. AbdelRaouf (2021), for instance, uses a revolutionary steganographic approach using the adaptable least significant bit (LSB) technique to hide data within images. While this method exhibits high image quality, it suffers from a relatively slower embedding rate. An interesting suggestion is the incorporation of encryption before embedding and compressing confidential message files to bolster security and attain a greater payload capacity. This highlights a recurring theme in the literature: the balance between payload capacity and security. Hussain et al.(2021) proposed an improved adaptive data concealment method that combines LSB and pixel value differencing (PVD) techniques, offering excellent invisibility and embeddability. However, the security aspect is left open, suggesting a need for encryption to enhance it. This trade-off between security and embedding capacity is a decisive consideration in steganography.

Murugan & Uthandipalayam Subramaniyam(2020) proposed a technique using the alpha factor to include data in the coefficient values of a picture and subjected it to a 2D-Haar discrete wavelet transform to create four sub-bands. The method offers embedded space and security compared to current approaches. However, it should be noted that the proposed method is complex. The domain of steganography and security holds a distinctive position in the realm of communication. Although it does not serve as a substitute for cryptography, it is intended to complement it. In multilayer steganography, Sahu & Swain (2020) introduced a dual-layer reversible information hiding (RIH) image steganography technique using modified LSB matching. This approach significantly increases payload while maintaining image imperceptibility.

The integration of security algorithms is suggested to further enhance data protection. This concept of multilayer steganography is intriguing, as it offers the potential for both increased capacity and security. Additionally, it can be optimized to reduce processing time. Another proposition was placed by Nie et al.(2019) introduced an approach combining Knight Tour algorithm with LSB as security layers for image steganography. The algorithm is used to find specific pixels within the cover picture to embed the encrypted secret message using LSB technique. The security technique was assessed using metrics like MSE, PSNR, and Chi-Squared Statistical Attack. The study found that the proposed scheme has higher resilience against steganalysis assaults compared to conventional LSB approaches, improving image security. However, the Knight Tour Algorithm has limitations in the dimensions of cover images, as it requires the image size to be divisible by 4 without residual.

To improve its use across cover images of varying sizes, further research should incorporate an additional steganography approach to enhance embedding capacity. The current method can only accommodate a maximum data size of 32.765KB, which is limited by available space. Abuzanouneh & Hadwan (2021) introduced a brand-new stenographic technology known as multi-stage protection employing pixel selection (MPPST). Which is reducing the detectability of secret files based on a complicated and random secret key containing numerous keys. Moreover, employing MPPST in a steganography system is crucial for hiding and retrieving secret data concealed within image files. The observed results for the relative entropy indicate that MPPST provides sufficient security to conceal secret messages and to decrease the size of the stego-image with a virtually imperceptible change that cannot be readily detected. The embedding probabilities provide evidence of the reliability and robustness of the MPPST security system against intruders and attackers.

Similarly, O. F. AbdelWahab et al. (2021) utilized an effective picture steganography method for concealing data to ensure secure data transfer. The encryption technique employed in this strategy involves the utilization of the RSA method to encrypt plain text. Subsequently, the encrypted text is then embedded into the YCbCr components of a picture by applying the LSB approach. The steganographic picture obtained is further subjected to compression techniques such as DWT, RLC, or Huffman coding to get a compressed steganographic image. The study reveals that Huffman coding is highly efficient and the best choice for compression purposes. The approach has a substantial payload coupled with a noteworthy level of image quality. Nevertheless, the system exhibits a high level of complexity.

Duan et al.(2020) Duan et al. (2020) developed a high-capacity image concealing method using elliptic curve cryptography (ECC) and deep neural networks. This method enhances data security on both grayscale and color images, but its complexity suggests room for optimization. The symbiotic relationship between cryptography and steganography provides heightened security, but it comes at the cost of complexity. The method's implementation highlights the need for further research in this area. Some studies incorporate multiple layers of security. Al-Shaarani & Gutub (2021) integrated matrix-based secret sharing, LSB and DWT steganography, and XOR encryption in preserving cover images. They found that the LSB method was more effective with small key sizes, while DWT was more effective with larger ones. The combination of XOR encryption and steganography enhanced share security without compromising quality.

Tauhid et al.(2019) Tauhid et al. (2019) propose a method that combines AES and LSB for secure data transmission. They use a DCT to encrypt the data within the spatial domain of the carrier picture, and the least significant bit (LSB) to include the secret information in the transform domain. An additional security layer is introduced through an XOR operation between encoded bits and carrier picture pixels, providing three levels of information protection and flawless decryption, but with limited embedding capacity. Zaheer et al.(2019) developed a system that exploits 3-bit planes for inserting information and uses DCT and thresholding to reduce the payload. The message image has been covered with a 2-bit error code to make it error-resistant. The findings indicate improved capacity and imperceptibility, and the recovered message image is of high quality and easily readable. However, the enhancement of the security of the procedure may be achieved via the utilization of an encryption algorithm.

Another approach to gaining traction is the hybridization of cryptographic and steganographic methods. Elhoseny et al.(2018) proposed a methodology for secure medical data transfer using 2D-DWT-1L or 2D-DWT-2L to disguise data and AES-RSA hybrid encryption for security. The approach achieved excellent image quality and data security; moreover, the DWT-2L method outperforms the DWT-1L method in terms of PSNR and MSE for colour and grayscale images. However, the complexity of the method still poses a concern. As articulated by Biswas et al.(2019) propose hybrid cryptography, which uses RSA and AES for encryption and LSB, a steganographic technique, to enhance security. They use histograms of cover pictures and stego images to demonstrate resistance to attack. The algorithm provides confidentiality, integrity, and authentication. However, the study lacks quantitative measurements to assess the efficacy of the system, making it difficult to determine if it is superior or comparable to traditional approaches in terms of quality. Adee & Mouratidis (2022) presented a data security paradigm for cloud data using AES, RSA cryptography, LSB and identity-based encryption to offer additional protection and fortify existing privacy and security challenges.

Furthermore, users could create backups of decryption outcomes, which allows for the secure sharing and transfer of encrypted data between authorized recipients, and the reduction of picture distortion enhances the level of data hiding within the image. However, achieving a higher payload requires executing a suitable compression method. In contrast, Widyawati et al.(2023) evaluated hybrid cryptography techniques, including ECDH-AES and RSA-AES, to ensure message security. They assessed their efficiency in terms of processing time, memory consumption, and security. The study found that ECDH-AES generally has reduced processing time and memory usage compared to RSA-AES. RSA-AES had processing times ranging from 0.03 seconds to 7 seconds, while ECDH-AES had processing times ranging from 0.003 seconds to 0.01 seconds. The minimum and maximum memory use for RSA-AES were 2.9 KB and 8.9 KB, respectively. ECDH-AES was considered better in terms of security due to the computational complexity of solving the logarithm problem on a discrete elliptic curve.

The described procedure employs a 2-3-4 paradigm, in which the insertion is carried out in a sequential manner for the red channel. The values of MSE and PSNR were found to be dependent on the size and variation of pixels. The results obtained were intermediate and contingent upon the images employed. However, the system is not strong against statistical attacks. Abood et al. (2019) introduced cryptography and steganography algorithms to enhance data communication security. AES-LSB techniques ensure secure transmission between sender and receiver in unsecured networks.

The encrypted text is hidden in images using the LSB algorithm, making it a secure and effective system. Performance evaluations using PSNR and MSE show no differences between the original and stego images. The quality of stego pictures increases with the spread picture size, reducing distortion. The proposed method is robust and effective for secure data communication. The reviewed studies emphasize the significance of combining steganography and cryptography to enhance data security, imperceptibility, and embedding capacity. Each approach has its advantages

and limitations, requiring careful consideration for specific use cases and file formats. Additionally, suggestions for introducing encryption algorithms to reinforce security are frequently made, reflecting the ongoing efforts to improve data protection in the domain of steganography and security.

Summarization Of Literature

In this section will illustrate the summarization of literature review, as shown below in table 3

Table 3. Summarization of Literature Review

Author, Reference	Cryptography Algorithm	Steganography Method	Another Method Employed	Dataset /Sampling	Limitation
AbdelRaouf, (2021)	-	Adaptable LSB	-	The cover image dataset is a USC-SIPI image with 256x256 pixels, 512x512 pixels, and 1024x1024 pixels as sizes. This picture has 24 bits per pixel for color and 8 bits per pixel for grayscale.	Good picture quality, slower embedding rate, which requires compression methods to attain a greater payload capacity. And enhance security by applying encryption algorithms before embedding method.
Hussain et al.(2021)	-	LSB PVD	-	standard UCID andUSC-SIPI image datasets	Considerable imperceptivity, good embedding capacity, less secure requires encryption algorithms to improve it, as well as tested only on grayscale images.
Murugan & Uthandipalayam Subramaniyam, (2020)	-	2D-Haar DWT	-	Both the cover image and the hidden image are identical in size (512 × 512) and type (JPEG). The photos are named mixedfruits.jpg, myna1.jpg, and sunflower.jpg, each with a resolution of 512 × 512.	High data storage capacity and excellent image imperceptibility, less secure requires encryption algorithms before embedding method to improve it and complex.
Sahu & Swain, (2020)	-	RIH LSB	-	USC–SIPI image databases	Enough payload, better image imperceptivity, less secure requires encryption algorithms to optimize it, didn't analyze on color images and the processing time is longer.
Nie et al.(2019)	-	LSB	Knight Tour Algorithm	used grayscale images Each image is 512x512 pixels in size.	Improve Security, limited space capacity of embedding in the cover image that require execute compression method. The data provided does not include any numerical results.

Alotaibi et al.(2019)	AES Hash function	LSB	-	MySQL database	The image has poor visual quality despite carrying a significant payload. less embedding space, which entails executing a suitable compression method.
O. F. AbdelWahab et al. (2021)	RSA	LSB	compression method (Huffman coding, RLE, or DWT)	Six color images have been calculated size 128x128 pixel	high quality, storage capacity and security. However, Complex and the encryption algorithm does not possess authentication verification
Duan et al.(2020)	ECC	DCT	Deep neural network	Analyzed on color and grayscale pictures	Secure, Increased capacity, Significant picture quality, Complex
Al-Shaarani & Gutub,(2021)	XOR encryption	LSB DWT	matrix-based secret sharing	50 photos taken from two separate datasets, including USC-SIPI	secure. However, using only XOR encryption to optimize security by applying a hybrid cryptography algorithm
Tauhid et al.(2019)	AES	DCT LSB replacement	-	Various forms of color and grayscale photos were utilized as the cover image.	Secure, Limited Embedding capacity
Zaheer, Qureshi, Rahman, et al. (2019)	-	DCT	Thresholding of the coefficients	grayscale images. Two cover images are (Baboon and Lena), which are both 512 by 512 pixels in size and the two images size 256 × 256 are selected for embedding as message images (Message Image Eagle and Message Image Roger).	improved capacity and imperceptibility, less secure requires encryption algorithms
Elhoseny et al.(2018)	AES RSA	D-DWT-1L or 2D-DWT-2L	-	DME eyes dataset DICOM dataset	Good image quality, Secure, Complex Low payload
Biswas et al.(2019)	AES RSA	LSB	-	-	provides confidentiality, integrity and authentication together. The lack of quantitative measurements hinders the evaluation of the system's efficacy compared to traditional methods, thereby limiting its comparison.
Adee & Mouratidis (2022)	AES RSA	LSB	-	Three distinct images with variable dimensions and color gradients. Within the collection of photographs, there existed one with a file size of 1.2 MB, a different one was 2.9 MB, and the biggest one was 7.2 MB.	Secure, less embedding which requires executing a suitable compression method on the data before hiding

Widyawati et al. (2023)	(ECDH-AES) vas (RSA-AES)	-	-	text sizes of 24, 61, 152, and 137 bytes	To enhance security, add two other layers: steganography and compression methods.
Wahab et al.(2021)	RSA	LSB	compression method (Huffman coding and DWT)	Color image in several formats such as jpeg, png, and bmp	Good payload and Considerable image quality ,The algorithm does not possess authentication verification.
Awadh et al. (2022)	AES	DWT LSB	-	There are 40 cover images of different sizes.	improves data security and system performance, but the encryption algorithm does not possess authentication verification.
M. Kumar et al. (2022)	AES	LSB	-	-	less embedding space, which requires executing a suitable compression method and the encryption algorithm does not possess authentication verification.
Chauhan et al. (2017)	XOR encryption	LSB	-	SIPI database	The system is not strong against statistical attacks and less secure which need to add another encryption algorithm.
Abood et al. (2019)	AES	LSB	-	cover pictures of different sizes and types (jpg, tiff, and png)	Secure, but the encryption algorithm does not possess authentication verification.

DISCUSSION AND RECOMMENDATIONS

The reviewed studies present an ongoing effort to achieve a balance between payload capacity, imperceptibility, image quality, and security within the field of steganography. Although certain approaches may demonstrate proficiency in one area, they may have deficiencies in other areas. There is an increasing consensus on the need of using encryption methods to enhance security, particularly inside mobile and cloud-based communication systems. Furthermore, the combination of cryptography with steganography is gaining popularity since it provides a comprehensive strategy to ensure data security. Scholars underscore the significance of integrating hybrid encryption with steganographic methods to guarantee the preservation of data confidentiality, integrity, and authenticity. One further obstacle is to the complexity of certain proposed methodologies, potentially restricting their widespread use. The availability of steganography tools that incorporate these sophisticated techniques is crucial for enhancing their accessibility among a broader user base. Furthermore, it is necessary to modify procedures to fit images of diverse sizes and dimensions. In a similar vein, this thesis proposes a new conceptual framework of steganography and cryptography. The subsequent recommendations derived from the review may prove valuable to research:

1. The integration of the domains of Cryptography and Steganography with the disciplines of Deep Learning and Machine Learning.
2. Implementation of a multi-layer model can be employed to enhance security measures for multimedia data. How does it enhance security measures.
3. Studying the trade-off between the security and efficiency of the hybrid algorithm and finding the right balance between these factors is an important consideration when choosing an encryption method.
4. Data compression techniques can be applied to both encrypted data and steganographic content to minimize storage demands and enhance the capacity of channels or networks.
5. Use strong hybrid cryptography and steganography techniques to enhance data security.

CONCLUSION

In this technology era, the major concern is data confidentiality, integrity, and authenticity. Cryptography and steganography have emerged as crucial techniques for securing data and communications. This paper has reviewed and discussed the concept of cryptography algorithms and steganography methods. In addition, this paper ambitions for a deeper comprehension of image steganography and its combination with encryption techniques to develop advanced multilayer security systems. The combination of cryptography and steganography provides a multi-faceted defense mechanism against prospective threats. By using encryption, the privacy of information can be preserved, while steganography increases the level of obscurity, making it tough for rivals to identify and intercept sensitive data. whereas most of the current image-steganography techniques still suffer from inadequacy in terms of security, payload limitations, image quality insufficiency, and complexity. Therefore, it is of great importance to develop effective image steganography methodologies that are combined with data encryption. By reducing complexity, this approach will improve image embedding capability, security and picture imperceptibility. Additionally, it will also provide resilience against various attacks.

Acknowledgement

This research is fully supported by SEED GRANT, SG-010-022023-FISE from Management and Science University, for the grant provided. Also, would like to convey our appreciation to Majoury Benghazi high institute for Engineering Technology for providing research scholarship to enhance this study.

REFERENCES

[1] O. Evsutin, A. Melman, and R. Meshcheryakov, “Digital steganography and watermarking for digital images: A review of current research directions,” *IEEE Access*, vol. 8, pp. 166589–166611, 2020, doi: 10.1109/ACCESS.2020.3022779.

[2] F. Hazzaa, A. M. Shabut, N. H. M. Ali, and M. Cirstea, “Security Scheme Enhancement for Voice over Wireless Networks,” *Journal of Information Security and Applications*, vol. 58, May 2021, doi: 10.1016/j.jisa.2021.102798.

[3] Musa. M. Yahaya and A. Ajibola, “Cryptosystem for Secure Data Transmission using Advance Encryption Standard (AES) and Steganography,” *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, pp. 317–322, Dec. 2019, doi: 10.32628/cseit195659.

[4] A. K. Agrahari, M. Sheth, and N. Praveen, “Comprehensive Survey on Image Stegnography Using LSB With AES In-depth study of various requirements in the process of embedding, encrypting and extracting of text data,” 2018. [Online]. Available: http://www.ripublication.com

[5] E. Hureib, A. Gutub, E. S. Bin Hureib, and A. A. Gutub, “Enhancing Medical Data Security via Combining Elliptic Curve Cryptography and Image Steganography,” 2020. [Online]. Available: https://www.researchgate.net/publication/344311992

[6] A. F. Osuolale, “Secure Data Transfer Over the Internet Using Image CryptoSteganography,” *Int J Sci Eng Res*, vol. 8, no. 12, pp. 1115–1121, Dec. 2017, doi: 10.14299/ijser.2017.12.002.

[7] A. Jan, S. A. Parah, M. Hussan, and B. A. Malik, “Double layer security using crypto-stego techniques: a comprehensive review,” Jan. 01, 2022, *Springer Science and Business Media Deutschland GmbH*. doi: 10.1007/s12553-021-00602-1.

[8] B. T. Ahmed, “A systematic overview of secure image steganography,” *International Journal of Advances in Applied Sciences*, vol. 10, no. 2, p. 178, Jun. 2021, doi: 10.11591/ijaas.v10.i2.pp178-187.

[9] A. Febryan, T. W. Purboyo, and R. E. Saputra, “Steganography Methods on Text, Audio, Image and Video: A Survey,” 2017. [Online]. Available: http://www.ripublication.com

[10] L. Aslam, A. Saeed, I. M. Qureshi, M. Amir, and W. Khan, “Novel image steganography based on preprocessing of secrete messages to attain enhanced data security and improved payload capacity,” *Traitement du Signal*, vol. 37, no. 1, pp. 129–136, 2020, doi: 10.18280/ts.370117.

[11] A. Khaldi, “Steganographic Techniques Classification According to Image Format,” *International Annals of Science*, vol. 8, no. 1, pp. 143–149, Nov. 2019, doi: 10.21467/ias.8.1.143-149.

[12] A. M. Ray, A. Sarkar, A. J. Obaid, and S. Pandiaraj, “IoT security using steganography,” in *Multidisciplinary Approach to Modern Digital Steganography*, IGI Global, 2021, pp. 191–210. doi: 10.4018/978-1-7998-7160-6.ch009.

[13] N. E. Touati and A. M. Lakhdar, “Self embedding digital watermark using hybrid method against compression attack,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 24, no. 2, pp. 864–870, Nov. 2021, doi: 10.11591/ijeecs.v24.i2.pp864-870.

[14] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, “Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research,” *Neurocomputing*, vol. 335, pp. 299–326, Mar. 2019, doi: 10.1016/j.neucom.2018.06.075.

[15] W. Akeel Awadh, A. Salah Hashim, and A. Khalaf Hamoud, "A Review of Various Steganography Techniques in Cloud Computing," 2019. [Online]. Available: https://ssrn.com/abstract=3621535
[16] A. Alsaidi, K. Al-lehaibi, H. Alzahrani, M. AlGhamdi, and A. Gutub, "Compression Multi-Level Crypto Stego Security of Texts Utilizing Colored Email Forwarding," *Journal of Computer Science & Computational Mathematics*, pp. 33–42, Sep. 2018, doi: 10.20967/jcscm.2018.03.002.
[17] A. Selvam and P. R, "A Study on Network Security and Cryptography A STUDY ON CRYPTOGRAPHY AND NETWORK SECURITY View project," Tamil Nadu, India, Jul. 2022. [Online]. Available: https://www.researchgate.net/publication/358242788
[18] D. Reis, X. Sharon Hu, S. Member, H. Geng, M. Niemier, and S. Member, "IMCRYPTO: An In-Memory Computing Fabric for AES Encryption and Decryption," *IEEE Trans Very Large Scale Integr VLSI Syst*, vol. 30, no. 5, pp. 553–565, 2022, [Online]. Available: https://www.researchgate.net/publication/356817991
[19] U. Larbi and B. Mhidi, "Cryptanalysis and improvement of multimodal data encryption by machine-learning based system," Networks and Multimedia, 2023. doi: 10.13140/RG.2.2.19267.37920.
[20] I. F. Ashari, A. W. Bhagaskara, J. M. Cakrawarty, and P. R. Winata, "Image Steganography Analysis Using GOST Algorithm and PRNG Based on LSB," *Techno.Com*, vol. 21, no. 3, pp. 700–713, Aug. 2022, doi: 10.33633/tc.v21i3.6331.
[21] M. S. Taha, M. S. Mohd Rahim, S. A. Lafta, M. M. Hashim, and H. M. Alzuabidi, "Combination of Steganography and Cryptography: A short Survey," in *IOP Conference Series: Materials Science and Engineering*, Institute of Physics Publishing, Jun. 2019. doi: 10.1088/1757-899X/518/5/052003.
[22] C. and Biswas, U. D. and Gupta, and Md. M. Haque, *An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography*. IEEE, 2019.
[23] S. Ramakrishnan, *Cryptographic and Information Security*. CRC Press, 2018. doi: 10.1201/9780429435461.
[24] N. Rashmi and K. Jyothi, *An Improved Method for Reversible Data Hiding Steganography Combined with Cryptography*. 2018.
[25] W. A. Awadh, A. S. Alasady, and A. K. Hamoud, "Hybrid information security system via combination of compression, cryptography, and image steganography," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 6, p. 6574, Dec. 2022, doi: 10.11591/ijece.v12i6.pp6574-6584.
[26] N. N. Mohamed, Y. M. Yussoff, M. A. Saleh, and H. Hashim, "Hybrid cryptographic approach for internet of things applications: A review," *Journal of Information and Communication Technology*, vol. 19, no. 3, pp. 279–319, Jul. 2020, doi: 10.32890/jict2020.19.3.1.
[27] M. Faheem, S. Jamel, A. Hassan, Z. A., N. Shafinaz, and M. Mat, "A Survey on the Cryptographic Encryption Algorithms," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 11, 2017, doi: 10.14569/ijacsa.2017.081141.
[28] M. E. Saleh, A. A. Aly, and F. A. Omara, "Data Security Using Cryptography and Steganography Techniques," 2016. [Online]. Available: www.ijacsa.thesai.org
[29] F. R. Shareef, "A novel crypto technique based ciphertext shifting," *Egyptian Informatics Journal*, vol. 21, no. 2, pp. 83–90, Jul. 2020, doi: 10.1016/j.eij.2019.11.002.
[30] M. Alaeian, Dānishgāh-i ʿIlm va Ṣanʿat-i Īrān, Iranian Society of Cryptology, and Institute of Electrical and Electronics Engineers, "Advantages and disadvantages of using cryptography in steganography," *2020 17th International ISC Conference on Information Security and Cryptology (ISCISC)*, pp. 88–94, Sep. 2020.
[31] M. Almazrooie, A. Samsudin, A. A. A. Gutub, M. S. Salleh, M. A. Omar, and S. A. Hassan, "Integrity verification for digital Holy Quran verses using cryptographic hash function and compression," *Journal of King Saud University - Computer and Information Sciences*, vol. 32, no. 1, pp. 24–34, Jan. 2020, doi: 10.1016/j.jksuci.2018.02.006.
[32] M. Alotaibi, D. Al-hendi, B. Alroithy, M. AlGhamdi, and A. Gutub, "Secure Mobile Computing Authentication Utilizing Hash, Cryptography and Steganography Combination," *Journal of Information Security and Cybercrimes Research*, vol. 2, no. 1, 2019, doi: 10.26735/16587790.2019.001.
[33] V. Cheval, C. Cremers, A. Dax, L. Hirschi, C. Jacomme, and S. Kremer, "Hash Gone Bad: Automated discovery of protocol attacks that exploit hash function weaknesses," 2023.
[34] M. I. Mihailescu and S. L. Nita, "Cryptography and Cryptanalysis in MATLAB_ Creating and Programming Advanced Algorithms-Hash Functions," in *Apress, Berkeley, CA*, 1st ed. edition., Spring, 2021, ch. 8, pp. 83–102.
[35] N. Q. B. Vo, T. T. Duy, Posts and Telecommunications Institute of Technology, Duy Tan University, IEEE Vietnam Section, and Institute of Electrical and Electronics Engineers, "Dual Image based LSB Steganography," in *IEEE*, 2018 2nd International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom), 2018, pp. 61–66.
[36] R. Din, R. Bakar, S. Utama, J. Jasmis, and S. J. Elias, "The evaluation performance of letter-based technique on text steganography system," *Bulletin of Electrical Engineering and Informatics*, vol. 8, no. 1, pp. 291–297, Mar. 2019, doi: 10.11591/eei.v8i1.1440.

[37] F. Q. Alyousuf, F. Qasim, A. Al-Yousuf, and R. Din, "Review on secured data capabilities of cryptography, steganography, and watermarking domain," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 17, no. 2, pp. 1053–1059, 2020, doi: 10.11591/ijeecs.v17.i2.pp1053-1059.
[38] S. Aliyu Ahmad, A. Baita Garko, and M. Sirajo Aliyu, "Full Paper SECURING TEXTUAL AND MULTIMEDIA DATA USING CRYPTOGRAPHY AND STEGANOGRAPHY ALGORITHM: A SYSTEMATIC REVIEW," in *Conference: Nigeria Computer Society (NCS) International ConferenceAt: Abeokuta - Ogun State, Nigeria*, 2022. [Online]. Available: https://www.researchgate.net/publication/363011974
[39] G. V. K. Murugan and R. Uthandipalayam Subramaniyam, "Performance analysis of image steganography using wavelet transform for safe and secured transaction," *Multimed Tools Appl*, vol. 79, no. 13–14, pp. 9101–9115, Apr. 2020, doi: 10.1007/s11042-019-7507-6.
[40] L. Negi, S. Kumar, and M. Bharti, "Strengthening Data Security of India using a mixed approach of Cryptography and Steganography Techniques: A Review," in *Proceedings - IEEE International Conference on Device Intelligence, Computing and Communication Technologies, DICCT 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 494–499. doi: 10.1109/DICCT56244.2023.10110086.
[41] S. Dhawan and R. Gupta, "Comparative Analysis of Domains of Technical Steganographic Techniques," in *IEEE*, 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), 2019, pp. 885–889. [Online]. Available: https://www.researchgate.net/publication/343713080
[42] S. Chauhan, Jyotsna, J. Kumar, and A. Doegar, "Multiple layer text security using variable block size cryptography and image steganography," in *2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT)*, 2017, pp. 1–7.
[43] S. Bandyopadhyay, "A Graphical Based Video Steganography Fluid Phase Equilibria View project," 2021, doi: 10.20944/preprints202105.0176.v1.
[44] M. Magdy, K. M. Hosny, N. I. Ghali, and S. Ghoniemy, "Security of medical images for telemedicine: a systematic review," *Multimed Tools Appl*, vol. 81, no. 18, pp. 25101–25145, Jul. 2022, doi: 10.1007/s11042-022-11956-7.
[45] X. Duan, D. Guo, N. Liu, B. Li, M. Gou, and C. Qin, "A New High Capacity Image Steganography Method Combined With Image Elliptic Curve Cryptography and Deep Neural Network," *IEEE Access*, vol. 8, pp. 25777–25788, 2020, doi: 10.1109/ACCESS.2020.2971528.
[46] M. Hussain, A. W. A. Wahab, Y. I. Bin Idris, A. T. S. Ho, and K. H. Jung, "Image steganography in spatial domain: A survey," *Signal Process Image Commun*, vol. 65, pp. 46–66, Jul. 2018, doi: 10.1016/j.image.2018.03.012.
[47] A. AbdelRaouf, "A new data hiding approach for image steganography based on visual color sensitivity," *Multimed Tools Appl*, vol. 80, no. 15, pp. 23393–23417, Jun. 2021, doi: 10.1007/s11042-020-10224-w.
[48] M. Zaheer *et al.*, "High Capacity Image Steganography Based on Prime Series Representation and Payload Redundancy Removal," *Journal of Information Assurance and Security*, vol. 14, no. 2, 2019, [Online]. Available: https://www.researchgate.net/publication/335292497
[49] O. F. A. AbdelWahab, A. A. M. Khalaf, A. I. Hussein, and H. F. A. Hamed, "Hiding data using efficient combination of RSA cryptography, and compression steganography techniques," *IEEE Access*, vol. 9, pp. 31805–31815, 2021, doi: 10.1109/ACCESS.2021.3060317.
[50] N. Sharma and U. Batra, "Performance analysis of compression algorithms for information security: A Review," *ICST Transactions on Scalable Information Systems*, p. 163503, Jul. 2018, doi: 10.4108/eai.13-7-2018.163503.
[51] G. Xin and P. Fan, "A lossless compression method for multi-component medical images based on big data mining," *Sci Rep*, vol. 11, no. 1, Dec. 2021, doi: 10.1038/s41598-021-91920-x.
[52] M. R. Kumar and M. N. Singh, "A survey based on Enhanced the Security of Image using the combined techniques of steganography and cryptography," Jan. 2020. [Online]. Available: https://ssrn.com/abstract=3563571
[53] M. Hussain, Q. Riaz, S. Saleem, A. Ghafoor, and K. H. Jung, "Enhanced adaptive data hiding method using LSB and pixel value differencing," *Multimed Tools Appl*, vol. 80, no. 13, pp. 20381–20401, May 2021, doi: 10.1007/s11042-021-10652-2.
[54] A. K. Sahu and G. Swain, "Reversible Image Steganography Using Dual-Layer LSB Matching," *Sens Imaging*, vol. 21, no. 1, Dec. 2020, doi: 10.1007/s11220-019-0262-y.
[55] S. A. Nie, G. Sulong, R. Ali, and A. Abel, "The use of least significant bit (LSB) and knight tour algorithm for image steganography of cover image," *International Journal of Electrical and Computer Engineering*, vol. 9, no. 6, pp. 5218–5226, 2019, doi: 10.11591/ijece.v9i6.pp5218-5226.
[56] K. I. M. Abuzanouneh and M. Hadwan, "Multi-Stage Protection using Pixel Selection Technique for Enhancing Steganography," 2021. [Online]. Available: https://www.researchgate.net/publication/350995778
[57] O. F. AbdelWahab, A. I. Hussein, H. F. Hamed, H. M. Kelash, and A. A. Khalaf, "Efficient combination of RSA cryptography, lossy, and lossless compression steganography techniques to hide data," *Procedia Comput Sci*, vol. 182, pp. 5–12, 2021.
[58] F. Al-Shaarani and A. Gutub, "Securing matrix counting-based secret-sharing involving crypto steganography," *Journal of King Saud University - Computer and Information Sciences*, Oct. 2021, doi: 10.1016/j.jksuci.2021.09.009.

[59] A. Tauhid, M. Tasnim, S. A. Noor, N. Faruqui, and M. A. Yousuf, “A Secure Image Steganography Using Advanced Encryption Standard and Discrete Cosine Transform,” *Journal of Information Security*, vol. 10, no. 03, pp. 117–129, 2019, doi: 10.4236/jis.2019.103007.
[60] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, “Secure Medical Data Transmission Model for IoT-Based Healthcare Systems,” *IEEE Access*, vol. 6, pp. 20596–20608, Mar. 2018, doi: 10.1109/ACCESS.2018.2817615.
[61] R. Adee and H. Mouratidis, “A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography,” *Sensors*, vol. 22, no. 3, Feb. 2022, doi: 10.3390/s22031109.
[62] L. Widyawati,) Husain,) Muhamad Azwar, M. Christian, and S. Girsang, “ANALISA PERBANDINGAN HYBRID CRYPTOGRAPHY RSA-AES DAN ECDH-AES UNTUK KEAMANAN PESAN,” *Jurnal Teknologi Informasi dan Komputer*, vol. 9, no. 2, 2023.
[63] M. Kumar, A. Soni, A. R. S. Shekhawat, and A. Rawat, “Enhanced Digital Image and Text Data Security Using Hybrid Model of LSB Steganography and AES Cryptography Technique,” in *Proceedings of the 2nd International Conference on Artificial Intelligence and Smart Energy, ICAIS 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 1453–1457. doi: 10.1109/ICAIS53314.2022.9742942.
[64] O. I. Al-Sanjary, O. A. Ibrahim, and K. Sathasivem, “A New Approach to Optimum Steganographic Algorithm for Secure Image,” in *2020 IEEE International Conference on Automatic Control and Intelligent Systems, I2CACIS 2020 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., Jun. 2020, pp. 97–102. doi: 10.1109/I2CACIS49202.2020.9140186.
[65] M. H. Abood, Z. K. Taha, and Z. K. Taha, “SECURE AND HIDDEN TEXT USING AES CRYPTOGRAPHY AND LSB STEGANOGRAPHY,” *Journal of Engineering Science and Technology*, vol. 14, no. 3, pp. 1434–1450, 2019, doi: 10.13140/RG.2.2.29786.80321.
[66] F. Al-Shaarani and A. Gutub, “Securing matrix counting-based secret-sharing involving crypto steganography,” *Journal of King Saud University - Computer and Information Sciences*, Oct. 2021, doi: 10.1016/j.jksuci.2021.09.009.
[67] M. Zaheer *et al.*, “High Capacity Image Steganography Based on Prime Series Representation and Payload Redundancy Removal,” *Journal of Information Assurance and Security*, 2019, [Online]. Available: https://www.researchgate.net/publication/335292497
[68] R A. A. Helmi, M. G. M. Johar and M. A. S. B. M. Hafiz, "Online Phishing Detection Using Machine Learning," 2023 1st International Conference on Advanced Innovations in Smart Cities (ICAISC), Jeddah, Saudi Arabia, 2023, pp. 1-4, doi: 10.1109/ICAISC56366.2023.10085377.
[69] M. H. Alkawaz, S. J. Steven and A. I. Hajamydeen, "Detecting Phishing Website Using Machine Learning," 2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA), Langkawi, Malaysia, 2020, pp. 111-114, doi: 10.1109/CSPA48992.2020.9068728.
[70] L. Dai, Md Gapar Md Johar, and Mohammed Hazim Alkawaz, “Review of Semi-Supervised Medical Image Segmentation based on the U-Net”, AJST, vol. 11, no. 1, pp. 147–154, May 2024, doi: 10.54097/gmhkht38.